LISTING OF THE CLAIMS

1. (Currently Amended) A method for protecting data generated by a keyboard, comprising the steps of:

reading data from a keypad of the keyboard;

reading an encryption seed from a device reader directly connected to the keyboard;

encrypting the read data using the encryption seed; and

directly transmitting the encrypted data from the keyboard to a computer wherein the encrypted data is not transmitted via the device reader to the computer and the computer and the device reader are different devices.

2. (Original) The method of claim 1 further comprises the steps of receiving the transmitted encrypted data by the computer; and

decrypting the received encrypted data by the computer.

3. (Original) The method of claim 1 wherein the step of transmitting comprises the step of using a wireless link over which the encrypted data is transmitted.

4. (Canceled)

5. (Canceled)

6. (Canceled)

7. (Previously Amended) The method of claim 1 wherein the step of reading the encryption seed comprises the step of enabling the device reader with a personal identification number.

8. (Canceled)

9. (Currently Amended) A method for protecting data generated by a keyboard, comprising the steps of:

generating a start signal by at least one of a special key on ~~keyboard~~ a keypad of the keyboard or multi-actuation of a number of keys on the keypad;

reading data from [a] the keypad ~~of the keyboard~~ following generation of the start signal wherein the read data and the start signal are distinct;

encrypting the read data in response to the start signal; ~~and~~

transmitting the encrypted data from the keyboard to a computer;

receiving a unique stop signal from the keypad;

stopping the encryption of the read data and transmission of the encrypted data from the keyboard to the computer in response to the stop signal.

10. (Canceled)

11. (Currently Amended) The method of claim ~~10~~ 9 wherein the step of receiving the stop signal comprises the step of generating the stop signal by at least one of a special key on keyboard or multi-actuation of a number of keys on the keypad.

12. (Canceled)

13. (Canceled)

14. (Canceled)

15. (Canceled)

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Canceled)

20. (Canceled)

21. (Canceled)

22. (Canceled)

23. (Canceled)

24. (Canceled)

25. (Canceled)

26. (Currently Amended) A keyboard for encrypting data before transmission to a computer directly connected to the keyboard via a link, comprising:

an interface connected to the link;

a memory;

a keypad for generating the data;

a device ~~reader~~ interface for reading a directly connected device reader to obtain a seed for an encryption routine wherein the device reader and the computer are different devices;

a processor for encrypting using the seed from the device reader the generated data from the keypad by execution of the encryption routine stored in the memory; and

directly transmitting the encrypted data to the computer via the interface and link bypassing the device reader and device interface.

27. (Original) The keyboard of claim 26 wherein the link is a wireless link.

28. (Canceled)

29. (Canceled)

30. (Original) The keyboard of claim 26 comprises a special key which when actuated causes the processor to at least start executing the encryption routine or stop executing the encryption routine.

31. (Currently Amended) A processor-readable medium for protecting data generated by a keyboard, comprising processor-executable instructions configured for:

reading data from a keypad of the keyboard;

reading an encryption seed from a device reader directly connected to the keyboard;

encrypting the read data using the encryption seed; and

directly transmitting the encrypted data from the keyboard to a computer wherein the encrypted data is not

transmitted via the device reader to the computer and the computer and the device reader are different devices.

32. (Original) The processor-readable medium of claim 31 wherein the transmitting comprises using a wireless link over which the encrypted data is transmitted.

33. (Canceled)

34. (Canceled)

35. (Canceled)

36. (Previously Amended) The processor-readable medium of claim 31 wherein the reading the encryption seed comprises enabling the device reader with a personal identification number.

37. (Canceled)

38. (Currently Amended) A processor-readable medium for protecting data generated by a keyboard, comprising processor-executable instructions configured for:

generating a start signal by at least one of a special key on ~~keyboard~~ a keypad of the keyboard or multi-actuation of a number of keys on the keypad;

reading data from [a] the keypad ~~of the keyboard~~ following generation of the start signal wherein the read data and the start signal are distinct;

encrypting the read data in response to the start signal; ~~and~~

transmitting the encrypted data from the keyboard to a computer;

receiving a unique stop signal from the keypad;

stopping the encryption of the read data and transmission of the encrypted data from the keyboard to the computer in response to the stop signal.

39. (Canceled)

40. (Currently Amended) The processor-readable medium of claim ~~39~~ 38 wherein the stop signal generated by at least one of a special key on keyboard or multi-actuation of a number of keys on the keypad.

41. (Canceled)

42. (Canceled)

43. (Canceled)

44. (Canceled)

45. (Canceled)

46. (Canceled)

47. (Canceled)

48. (Canceled)